INTERNATIONAL STANDARDIZED PROFILE

ISO/IEC ISP 10611-4

Second edition
1997-12-15

Information technology — International Standardized Profiles AMH1n — Message Handling Systems — Common Messaging —

Part 4:
AMH12 and AMH14 — MTS Access (P3) and MTS 94 Access (P3)

Technologies de l'information — Profils normalisés internationaux AMH1n — Systèmes de messagerie — Messagerie commune —

Partie 4: AMH12 et AMH14 — Accès à MTS (P3) et accès à MTS 94 (P3)

Reference number
ISO/IEC ISP 10611-4:1997(E)

Contents

Page

Foreword iii

Introduction iv

1 Scope 1

2 Normative references 2

3 Definitions 3

4 Abbreviations 4

5 Conformance 5

Annexes

A ISPICS Proforma for ISO/IEC ISP 10611-4 (AMH12 and AMH14) 7

B Amendments and corrigenda 54

C Bibliography 55

Information technology – International Standardized Profiles AMH1n – Message Handling Systems – Common Messaging –

Part 4: AMH12 and AMH14 – MTS Access (P3) and MTS 94 Access (P3)

1 Scope

1.1 General

This part of ISO/IEC ISP 10611 covers access to a Message Transfer System (MTS) using the P3 MTS Access Protocol (see also figure 1). These specifications form part of the Common Messaging application functions, as defined in the parts of ISO/IEC ISP 10611, which form a common basis for content type-dependent International Standardized Profiles for MHS that will be developed.

An MTA or a MTS-user which conforms to profile AMH12 as specified in this part of ISO/IEC ISP 10611 shall support a 'mts-access' application context and for the MTA also 'mts-forced-access' application context . The MTA or the MTS-user may additionally conform to profile AMH14 as specified in this part of ISO/IEC ISP 10611 shall support the 'mts-access-94' and 'mts-forced-access-94' application contexts.

1.2 Position within the taxonomy

This part of ISO/IEC ISP 10611 is the fourth part of a multipart ISP identified in ISO/IEC TR 10000-2 as "AMH1, Message Handling Systems - Common Messaging".

This part of ISO/IEC ISP 10611 specifies the following profiles:

AMH12 - MTS Access (P3)

AMH14 - MTS-94 Access (P3)

The AMH12 and AMH14 profiles may be combined with any T-Profiles (see ISO/IEC TR 10000) specifying the OSI connection-mode Transport service.

1.3 Scenario

The model used is one of access to an MTS by an MTS-user - specifically, the intercommunication between a message transfer agent (MTA) and an MTS-user using the P3 protocol, as shown in figure 1.

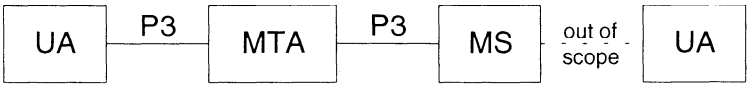

Figure 1 - AMH12 and AMH14 scenario

The AMH12 and AMH14 profiles covers all aspects of the MTS Abstract Service, as defined in clause 8 of ISO/IEC 10021-4, when realized using the P3 protocol.

The OSI upper layer services and protocols to support the Message Handling Systems functions covered by the AMH12 profile are specified in the set of standards identified in table 1.

Table 1 - AMH12 profile model

Application Layer	MHS	ISO/IEC 10021-6
	ROSE	see ISO/IEC ISP 10611-2
	RTSE	see ISO/IEC ISP 10611-2
	ACSE	see ISO/IEC ISP 10611-2
Presentation Layer		see ISO/IEC ISP 10611-2
Session Layer		see ISO/IEC ISP 10611-2

2 Normative references

The following documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC ISP 10611. At the time of publication, the editions indicated were valid. All documents are subject to revision, and parties to agreements based on this part of ISO/IEC ISP 10611 are warned against automatically applying any more recent editions of the documents listed below, since the nature of references made by ISPs to such documents is that they may be specific to a particular edition. Members of IEC and ISO maintain registers of currently valid International Standards and ISPs, and the Telecommunications Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

Amendments and corrigenda to the base standards referenced are listed in annex B.

NOTES

1 - References in the body of this part of ISO/IEC ISP 10611 to specific clauses of ISO/IEC documents shall be considered to refer also to the corresponding clauses of the equivalent ITU-T Recommendations (as noted below) unless otherwise stated.

2 - Informative references are found in annex E.

ISO/IEC TR 10000-1:—[1], *Information technology - Framework and taxonomy of International Standardized Profiles - Part 1: General principles and documentation framework.*

ISO/IEC TR 10000-2:—[1], *Information technology - Framework and taxonomy of International Standardized Profiles - Part 2: Principles and Taxonomy for OSI profiles.*

ITU-T Recommendation F.400/X.400 (1996), *Message Handling Systems - System and service overview.*

ISO/IEC 10021-1:—[2], *Information technology - Message Handling Systems (MHS): System and service overview [see also ITU-T Recommendation F.400/X.400].*

ITU-T Recommendation X.402 (1995) | ISO/IEC 10021-2: 1996, *Information technology - Message Handling Systems (MHS): Overall architecture.*

ITU-T Recommendation X.411 (1995) | ISO/IEC 10021-4: 1997, *Information technology - Message Handling Systems (MHS) - Message transfer system: Abstract service definition and procedures.*

ITU-T Recommendation X.419 (1995) | ISO/IEC 10021-6: 1996, *Information technology - Message Handling Systems (MHS): Protocol specifications.*

[1] To be published. (Revision of ISO/IEC 10000:1995)
[2] To be published. (Revision of ISO/IEC 10021-1:1994)

ISO/IEC ISP 10611-1: 1997, *Information technology - International Standardized Profiles AMH1n - Message Handling Systems - Common Messaging - Part 1: MHS Service Support.*

ISO/IEC ISP 10611-2: 1997, *Information technology - International Standardized Profiles AMH1n - Message Handling Systems - Common Messaging - Part 2: Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MHS.*

3 Definitions

For the purposes of this part of ISO/IEC ISP 10611, the following definitions apply.

Terms used in this part of ISO/IEC ISP 10611 are defined in the referenced base standards; in addition, the following terms are defined.

3.1 General

3.1.1 Basic requirement: an Element of Service, protocol element, procedural element or other identifiable feature specified in the base standards which is required to be supported by all MHS implementations.

3.1.2 Functional group: a specification of one or more related Elements of Service, protocol elements, procedural elements or other identifiable features specified in the base standards which together support a significant optional area of MHS functionality.

NOTE - A functional group can cover any combination of MHS features specified in the base standards for which the effect of implementation can be determined at a standardized external interface - i.e. via a standard OSI communications protocol (other forms of exposed interface, such as a standardized programmatic interface, are outside the scope of this version of ISO/IEC ISP 10611).

3.2 Support classification

To specify the support level of operations, arguments, results and other protocol features for this part of ISO/IEC ISP 10611, the following terminology is defined.

3.2.1 Static capability

The following classifications are used in this part of ISO/IEC ISP 10611 to specify static conformance requirements - i.e. capability.

In the case of arguments and results (protocol elements), the classification is relative to that of the containing element, if any. Where the constituent elements of a non-primitive element are not individually specified, then each shall be considered to have the classification of that element. Where the range of values to be supported for an element is not specified, then all values defined in the MHS base standards shall be supported.

3.2.1.1 mandatory full support (m): the element or feature shall be fully supported. An implementation shall be able to generate the element, and/or receive the element and perform all associated procedures (i.e. implying the ability to handle both the syntax and the semantics of the element) as relevant, as specified in the MHS base standards. Where support for origination (generation) and reception are not distinguished, then both capabilities shall be assumed.

3.2.1.2 mandatory minimal support (m-): the element shall be supported. However, an implementation is only required to be able to copy the syntax of the element to the corresponding element of a message, probe or report for onward transfer or delivery, as appropriate, according to the procedures as specified in the MHS base standards, unless further qualified for the output envelope in question elsewhere in this multipart ISP (i.e. the classification of the output envelope takes precedence). An implementation is not required to be able to take any explicit action based on the semantics of such an element other than to treat the element as supported for criticality purposes. An implementation is not required to be able to originate such an element.

NOTE - The m- classification is designed to distinguish those cases where the MHS base standards define more than one level of functionality and the minimum required level of support in this profile is the minimum functionality defined in the

base standards. Where the only functionality defined in the base standards is copying the element as described above, then the m classification is used in preference to m-.

3.2.1.3 optional support (o): an implementation is not required to support the element or feature. If support is claimed, the element shall be treated as if it were specified as mandatory support. If support for origination is not claimed, then the element is not generated and, in the case of non-support of a critical extension by an MTA implementation on delivery, shall cause a non-delivery notification to be returned. If support for reception is not claimed, and the element is an argument, then an implementation may ignore a non-critical extension on delivery but shall otherwise generate an appropriate error indication. If support for reception is not claimed, and the element is a result, then the element may be ignored. If support of an operation as a responder is not claimed, then an appropriate error indication shall be generated (as a minimum, a ROSE reject shall be generated).

3.2.1.4 conditional support (c): the element shall be supported under the conditions specified in this part of ISO/IEC ISP 10611. If these conditions are met, the element shall be treated as if it were specified as mandatory support. If these conditions are not met, the element shall be treated as if it were specified as optional support (unless otherwise stated).

3.2.1.5 out of scope (i): the element is outside the scope of this part of ISO/IEC ISP 10611 - i.e. it will not be the subject of an ISP conformance test.

3.2.1.6 not applicable (–): the element is not applicable in the particular context in which this classification is used.

3.2.2 Dynamic behaviour

The above classifications are used in this part of ISO/IEC ISP 10611 to specify static conformance requirements (i.e. capability); dynamic conformance requirements (i.e. behaviour) are as specified in the MHS base standards. However, in a few cases it has been necessary to specify additional dynamic conformance requirements in this profile. These are specified using a second classification code for an element, as follows.

NOTE - Subclause 6.7 of ISO/IEC TR 10000-1 states that a profile shall not introduce a constraint on dynamic behaviour on reception. However, in the case of MHS security (at least), the base standards define a suitable error indication to cover the breach of a security policy but do not specify the precise conditions under which such error indication shall be used. Any such specification in a profile is thus a legitimate qualification of the base standards rather than a modification of such provisions.

3.2.2.1 required (r): the element shall always be present. An implementation shall ensure that the element is always generated or otherwise used, as appropriate. Absence of the element on reception shall result in termination or rejection of the communication with an appropriate error indication as specified in the MHS base standards.

3.2.2.2 excluded (x): the element shall never be present. An implementation shall ensure that the element is never generated or otherwise used, as appropriate. Presence of the element on reception shall result in termination or rejection of the communication with an appropriate error indication as specified in the MHS base standards.

NOTE - It is recognized that some implementations may be required to exclude even a static capability in such cases, but such considerations are outside the scope of this profile. Any elements which are specified as excluded (x) in this profile are thus also specified as out of scope (i) in terms of static capability.

4 Abbreviations

AMH	Application Message Handling
ASN.1	Abstract Syntax Notation One
CV	Conversion
DC	Delivery Constraints
DIR	Use of Directory

DL	Distribution List
EoS	Element of Service
FG	Functional group
ISP	International Standardized Profile
LD	Latest Delivery
MHS	Message Handling Systems
MS	Message store
MTA	Message transfer agent
OSI	Open Systems Interconnection
PD	Physical Delivery
RD	Restricted Delivery
RED	Redirection
RED2	Redirection Instructions
RoC	Return of Content
SEC	Security
SPP	Simple Protected Password
UA	User agent

Support level for protocol elements and features (see 3.2):

m	mandatory full support
m-	mandatory minimal support
o	optional support
c	conditional support
i	out of scope
–	not applicable
r	required
x	excluded

5 Conformance

This part of ISO/IEC ISP 10611 states requirements upon implementations to achieve interworking. A claim of conformance to this part of ISO/IEC ISP 10611 is a claim that all requirements in the relevant base standards are satisfied, and that all requirements in the following clauses and in annex A of this part of ISO/IEC ISP 10611 are satisfied. Annex A states the relationship between these requirements and those of the base standards.

5.1 Conformance statement

For each implementation claiming conformance to profile AMH12 as specified in this part of ISO/IEC ISP 10611, a PICS shall be made available stating support or non-support of each option identified in this part of ISO/IEC ISP 10611.

The scope of conformance to profiles AMH12 and AMH14 covers both MTAs and MTS-users. A claim of conformance to profiles AMH12 and/or AMH14 shall state whether the implementation claims conformance as an MTA, as a UA, or as an MS which is not co-located with an MTA. The claim shall also state if the implementation conform to profiles AMH12 and/or AMH14.

5.2 MHS conformance

This part of ISO/IEC ISP 10611 specifies implementation options or selections such that conformant implementations will satisfy the conformance requirements of ISO/IEC 10021 and the ITU-T X.400 Recommendations.

Implementations conforming to profile AMH12 as specified in this part of ISO/IEC ISP 10611 shall implement all the mandatory support (m or m-) features identified as basic requirements in annex A except those features that are components of an unimplemented optional feature. It shall be stated which optional support (o) features are implemented.

For implementations conforming to profiles AMH12 and/or AMH14 as specified in this part of ISO/IEC ISP 10611, it shall be stated whether or not they support any of the optional functional groups as specified in ISO/IEC ISP 10611-1 which are applicable to the scope of this profile and to the role (i.e. MTA or MTS-user) for which conformance is claimed. For each functional group for which support is claimed, an implementation shall implement all the mandatory support (m or m-) features identified for that functional group in annex A except those features that are components of an unimplemented optional feature. It shall be stated which optional support (o) features are implemented.

Implementations shall support the procedures associated with supported protocol elements as specified in the base standards and as further specified in ISO/IEC ISP 10611-1. The MHS Elements of Service corresponding to such procedures are indicated in annex A of ISO/IEC ISP 10611-1.

For implementations conforming to profiles AMH12 and/or AMH14 as specified in this part of ISO/IEC ISP 10611, the P3 application context(s) for which conformance is claimed shall be stated.

5.3 Underlying layers conformance

Implementations conforming to profiles AMH12 and/or AMH14 as specified in this part of ISO/IEC ISP 10611 shall also conform to ISO/IEC ISP 10611-2 in accordance with the P3 application context(s) for which conformance is claimed.

Annex A[1]

(normative)

ISPICS Proforma

for ISO/IEC ISP 10611-4 (AMH12 and AMH14)

In the event of a discrepancy becoming apparent in the body of this part of ISO/IEC ISP 10611 and the tables in this annex, this annex is to take precedence.

Clause A.1 specifies the basic requirements for conformance to profiles AMH12 and AMH14. Clause A.2 specifies additional requirements to those specified in A.1 for each of the optional functional groups if conformance to such a functional group is claimed. Clause A.3 allows additional information to be provided for certain aspects of an implementation where no specific requirements are included in ISO/IEC ISP 10611. All three clauses shall be completed as appropriate.

In each table, the "Base" column reflects the level of support required for conformance to the base standard and the "Profile" column specifies the level of support required by this ISP (using the classification and notation defined in 3.2).

The generic term "MTS-user" is used in the tables in this annex where the distinction between different types of MTS-user is not significant. Where a column is headed "UA", then an MS is only required to be able to pass through such elements transparently between a UA and the MTA.

The "Ref" column is provided for cross-referencing purposes. The notation employed for references also indicates composite elements which contain sub-elements (a sub-element reference is prefixed by the reference of the composite element).

The "Support" column is provided for completion by the supplier of the implementation as follows:

Y	the element or feature is fully supported (i.e. satisfying the requirements of the m profile support classification)
Y-	the element or feature is minimally supported (i.e. satisfying the requirements of the m-profile support classification)
N	the element or feature is not supported, further qualified to indicate the action taken on receipt of such an element as follows: ND - the element is discarded/ignored NR - the PDU is rejected (with an appropriate error indication where applicable)
– or blank	the element or feature is not applicable (i.e. a major feature or composite protocol element which includes this element or feature is not supported or is minimally supported)

[1] **Copyright release for ISPICS proformas**
Users of this International Standardized Profile may freely reproduce the ISPICS proforma in this annex so that it can be used for its intended purpose and may further publish the completed ISPICS.

A.0 Identification of the implementation

A.0.1 Identification of PICS

Ref	Question	Response
1	Date of statement (YYYY-MM-DD)	
2	PICS serial number	
3	System conformance statement cross reference	

A.0.2 Identification of IUT

Ref	Question	Response
1	Implementation name	
2	Implementation version	
3	Hardware name	
4	Hardware version	
5	Operating system name	
6	Operating system version	
7	Special configuration	
8	Other information	

A.0.3 Identification of supplier

Ref	Question	Response
1	Organization name	
2	Contact name(s)	
3	Address	
4	Telephone number	
5	Telex number	
6	Fax number	
7	E-mail address	
8	Other information	

A.0.4 Identification of protocol

Ref	Question	Response
1	Title, reference number and date of publication of the protocol standard	
2	Protocol version(s)	not applicable
3	Addenda/amendments/corrigenda implemented	
4	Defect reports implemented	not applicable

A.0.5 Type of implementation

Ref	Implementation Type	Response
1	MTS-user (UA or MS)	
2	MTA	

NOTE - A separate PICS shall be completed for each implementation type for which conformance is claimed.

A.0.6 Global statement of conformance

Ref	Question	Response
1	Are all mandatory base standards requirements implemented?	

A.0.7 Statement of profile conformance

Ref	Question	Response	Comments
1	profiles implemented		
1.1	Are all mandatory requirements of profile AMH12 implemented?		
1.2	Are all mandatory requirements of profile AMH14 implemented?		
2	Are all mandatory requirements of any of the following optional functional groups implemented?		
2.1	Conversion (CV)		only applicable in the case of an MTA
2.2	Distribution List (DL)		only applicable in the case of an MTA
2.3	Physical Delivery (PD)		not applicable in the case of an MS
2.4	Redirection (RED)		only applicable in the case of an MTA
2.5	Latest Delivery (LD)		not applicable in the case of an MS
2.6	Return of Content (RoC)		
2.7	Security (SEC)		class(es):
2.8	Use of Directory (DIR)		not applicable in the case of an MS
2.9	Simple Protected Password (SPP)		
2.10	Redirection Instructions (RED2)		not applicable in the case of an MS
2.11	Delivery Constraints (DC)		not applicable in the case of an MS
2.12	Restricted Delivery (RD)		not applicable in the case of an MS

A.1 Basic requirements

A.1.1 Supported application contexts

Ref	Application Context	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	mts-access-88	o	c1	o4	c1,4		
2	mts-forced-access-88	o	c1	o4	c1,4		
3	mts-reliable-access-88	o	o	o5	o5		
4	mts-forced-reliable-access-88	o	o	o5	o5		
5	mts-access-94	o	c2	o4	c2,4		
6	mts-forced-access-94	o	c2	o4	c2,4		
7	mts-reliable-access-94	o	c3	o5	c3,4		
8	mts-forced-reliable-access-94	o	c3	o5	c3,4		

c1 - if conformance to AMH12 is claimed then m else o.

c2 - if conformance to AMH14 is claimed then m else n/a.

c3 - if conformance to AMH14 is claimed then o else n/a.

c4 - If either of mts-access or mts-forced-access application contexts is supported, then shall both of them for that "year" be supported.

c5 - If either of mts-reliable-access or mts-forced-reliable-access application contexts is supported, then shall all four contexts for that "year" be supported.

A.1.2 Supported operations

A.1.2.1 Bind and Unbind

Ref	Operation	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	MTSBind access	m	m	m	m		see A.1.3.1
2	MTSUnbind access	m	m	m	m		
3	MTSBind forced access	m	m	m	m		see A.1.3.1
4	MTSUnbind forced access	m	m	m	m		

A.1.2.2 Message Submission Service Element (MSSE)

Ref	Operation	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	MessageSubmission	m	m	m	m		see A.1.3.2
2	ProbeSubmission	o	o	m	m		see A.1.3.3
3	CancelDeferredDelivery	o	o	m	m		see A.1.3.4
4	SubmissionControl	o	o	o	o		see A.1.3.5

NOTE - If the MTS-user is an MS, then the requirement is only to be able to pass through these operations (i.e. between the MTA and a local or remote UA) unaltered.

A.1.2.3 Message Delivery Service Element (MDSE)

Ref	Operation	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	MessageDelivery	m	m	m	m		see A.1.3.6
2	ReportDelivery	m	m	m	m		see A.1.3.7
3	DeliveryControl	o	o	m	m		see A.1.3.8

A.1.2.4 Message Administration Service Element (MASE)

Ref	Operation	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	Register	o	o	o	o		see A.1.3.9
2	ChangeCredentials (MTA to UA)	o	o	o	o		see A.1.3.10
3	ChangeCredentials (UA to MTA)	o	o	o	o		see A.1.3.10

NOTE - For a UA or MTA, some or all of the services and functionality supported by these operations may be implemented by other means as a local matter.

A.1.3 Operation arguments/results

A.1.3.1 MTSBind

Ref	Element	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	initiator-name	m	m	m	m		
1.1.1	user-agent	c3	c3	c3	c3		see A.1.10.b
1.1.2	mTA	c4	c4	c4	c4		see A.1.10.b
1.1.3	message-store	c5	c5	c3	c3		see A.1.10.b
1.2	messages-waiting	o	c1	o	c1		
1.3	initiator-credentials	m	m	m	m		
1.3.1	simple	m	m	m	m		
1.3.1.1	octet-string	o	m	o	m		
1.3.1.2	ia5-string	o	o	o	o		
1.3.2	strong	o	o	o	o		
1.3.2.1	bind-token	m	m	m	m		see A.1.9/9
1.3.2.2	certificate	o	o	o	o		
1.3.3	protected	c8	c7	c8	c7		
1.3.3.1	signature	m	m	m	m		
1.3.3.1.1	password	o	m	o	m		
1.3.3.1.2	time1	o	o	o	o		
1.3.3.1.3	time2	o	m	o	m		
1.3.3.1.4	random1	o	m	o	m		
1.3.3.1.5	random2	o	o	o	o		
1.3.3.2	time1	o	o	o	o		
1.3.3.3	time2	o	m	o	m		
1.3.3.4	random1	o	o	o	o		
1.3.3.5	random2	o	o	o	o		

1.4	security-context	o	o	o	o		see A.1.9/3
1.5	extensions	c8	c7	c8	c7		
2	RESULT						
2.1	responder-name	m	m	m	m		
2.1.1	user-agent	c4	c4	c4	c4		see A.1.10.b
2.1.2	mTA	c3	c3	c3	c3		see A.1.10.b
2.1.3	message-store	c6	c6	c4	c4		see A.1.10.b
2.2	messages-waiting	o	c2	o	c2		
2.3	responder-credentials	m	m	m	m		
2.3.1	simple	m	m	m	m		
2.3.1.1	octet-string	o	m	o	m		
2.3.1.2	ia5-string	o	o	o	o		
2.3.2	strong	o	o	o	o		
2.3.2.1	bind-token	m	m	m	m		
2.3.2.1.1	signature-algorithm-identifier	m	m	m	m		
2.3.2.1.2	name	m	m	m	m		
2.3.2.1.3	time	m	m	m	m		
2.3.2.1.4	signed-data	o	o	o	o		
2.3.2.1.5	encryption-algorithm-identifier	o	o	o	o		
2.3.2.1.6	encrypted-data	o	o	o	o		
2.3.3	protected	c8	c7	c8	c7		
2.3.3.1	signature	m	m	m	m		
2.3.3.1.1	password	o	m	o	m		
2.3.3.1.2	time1	o	o	o	o		
2.3.3.1.3	time2	o	m	o	m		
2.3.3.1.4	random1	o	m	o	m		
2.3.3.1.5	random2	o	o	o	o		
2.3.3.2	time1	o	o	o	o		

2.3.3.3	time2	o	m	o	m		
2.3.3.4	random1	o	o	o	o		
2.3.3.5	random2	o	o	o	o		
2.4	extensions	c8	c7	c8	c7		

c1 - if the MTA is the initiator then o else –

c2 - if the MTS-user is the initiator then o else –

c3 - if the MTS-user is the initiator then m else –

c4 - if the MTA is the initiator then m else –

c5 - if the MTS-user is a MS and is the initiator then m else –

c6 - if the MTS-user is a MS and the MTA is the initiator then m else –

c7 - if conformance to AMH14 is claimed then o else –

c8 - if any access-94 application context is supported (A.1.1 items 5, 6, 7 or 8) then o else –

A.1.3.2 MessageSubmission

Ref	Element	UA		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	envelope	m	m	m	m		see A.1.4
1.2	content	m	m	m	m		
2	RESULT						
2.1	message-submission-identifier	m	m	m	m		see A.1.8/1
2.2	message-submission-time	m	m	m	m		
2.3	content-identifier	o	c1	m	m		
2.4	extensions	m	m	m	m		see A.1.9/1
2.4.1	originating-MTA-certificate	o	i	o	i		
2.4.2	proof-of-submission	o	i	o	i		see A.1.9/7
2.4.3	extensions	c3	c2	c3	c2		

c1 - if supported in message submission envelope then m else –

c2 - if conformance to AMH14 is claimed then o else –

c3 - if any access-94 application context is supported (A.1.1 items 5, 6, 7 or 8) then o else –

A.1.3.3 ProbeSubmission

Ref	Element	UA		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	envelope	m	m	m	m		see A.1.5
2	RESULT						
2.1	probe-submission-identifier	m	m	m	m		see A.1.8/1
2.2	probe-submission-time	m	m	m	m		
2.3	content-identifier	o	c1	m	m		
2.4	PrivateExtensions	c3	c2	c3	c2		

c1 - if supported in probe submission envelope then m else –

c2 - if conformance to AMH14 is claimed then o else –

c3 - if any access-94 application context is supported (A.1.1 items 5, 6, 7 or 8) then o else –

A.1.3.4 CancelDeferredDelivery

Ref	Element	UA		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	message-submission-identifier	m	m	m	m		see A.1.8/1
2	RESULT						
2.1	NULL	m	m	m	m		

A.1.3.5 SubmissionControl

Ref	Element	UA		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	controls	m	m	m	m		
1.1.1	restrict	m	m	o	m		
1.1.2	permissible-operations	m	m	o	o		
1.1.3	permissible-maximum-content-length	m	m	o	o		
1.1.4	permissible-lowest-priority	m	m	o	o		
1.1.5	permissible-security-context	o	o	o	o		see A.1.9/3
2	RESULT						
2.1	waiting	m	m	m	m		
2.1.1	waiting-operations	o	o	m	m		
2.1.2	waiting-messages	o	o	m	m		
2.1.3	waiting-content-types	o	o	m	m		
2.1.4	waiting-encoded-information-types	o	o	m	m		see A.1.8/3

A.1.3.6 MessageDelivery

Ref	Element	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	(envelope)	m	m	m	m		see A.1.6
1.2	content	m	m	m	m		
2	RESULT						
2.1	recipient-certificate	o	o	o	o		
2.2	proof-of-delivery	o	o	o	o		see A.1.9/6
2.3	extensions	c1	c2	c1	c2		

c1 - if any access-94 application context is supported (A.1.1 items 5, 6, 7 or 8) then o else –
c2 - if conformance to AMH14 is claimed then o else –

A.1.3.7 ReportDelivery

Ref	Element	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	(envelope)	m	m	m	m		see A.1.7
1.2	returned-content	o	c1	o	c1		
2	RESULT						
2.1	NULL	c2	c4	c2	c4		
2.2	extensions	c3	c5	c3	c5		

c1 - if supported in message submission envelope then m else –

c2 - if any access-88 application context is supported (A.1.1 items 1, 2, 3 or 4) then m else o

c3 - if any access-94 application context is supported (A.1.1 items 5, 6, 7 or 8) then o else –

c4 - if conformance to AMH12 is claimed then m else –

c5 - if conformance to AMH14 is claimed then o else –

A.1.3.8 DeliveryControl

Ref	Element	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	controls	m	m	m	m		
1.1.1	restrict	m	m	m	m		
1.1.2	permissible-operations	o	o	m	m		
1.1.3	permissible-maximum-content-length	o	o	m	m		
1.1.4	permissible-lowest-priority	o	o	m	m		
1.1.5	permissible-content-types	o	o	m	m		
1.1.6	permissible-encoded-information-types	o	o	m	m		if conformance to AMH12 is claimed see A.1.8/3
1.1.6.1	unacceptable-eits	c1	c3	c1	c3		
1.1.6.2	acceptable-eits	c1	c3	c1	c3		

1.1.6.3	exclusively-acceptable-eits	c1	c2	c1	c2		
1.1.7	permissible-security-context	o	o	o	o		see A.1.9/3
1.2	extensions	c1	c2	c1	c2		
2	RESULT						
2.1	waiting	m	m	m	m		
2.1.1	waiting-operations	m	m	o	o		
2.1.2	waiting-messages	m	m	o	o		
2.1.3	waiting-content-types	m	m	o	o		
2.1.4	waiting-encoded-information-types	m	m	o	o		see A.1.8/3
2.2	extensions	c1	c2	c1	c2		

c1 - if any access-94 application context is supported (A.1.1 items 5, 6, 7 or 8) then o else –

c2 - if conformance to AMH14 is claimed then o else –

c3 - if conformance to AMH14 is claimed then m else –

A.1.3.9 AMH12 Register

This classification applies only to the AMH12 context. (The AMH14 register operation is specified in A.1.3.11)

Ref	Element	UA		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	user-name	o	o	o	o		see A.1.10.b
1.2	user-address	o	o	o	o		
1.3	deliverable-encoded-information-types	o	o	o	m		see A.1.8/3
1.4	deliverable-maximum-content-length	o	o	o	m		
1.5	default-delivery-controls	o	o	o	o		
1.5.1	restrict	o	o	o	m		
1.5.2	permissible-operations	o	o	o	m		
1.5.3	permissible-maximum-content-length	o	o	o	m		
1.5.4	permissible-lowest-priority	o	o	o	m		

1.5.5	permissible-content-types	o	o	o	m		
1.5.6	permissible-encoded-information-types	o	o	o	m		see A.1.8/3
1.6	deliverable-content-types	o	o	o	m		
1.7	labels-and-redirections	o	o	o	o		
1.7.1	user-security-label	o	o	o	o		see A.1.9/3
1.7.2	recipient-assigned-alternate-recipient	o	o	o	o		
2	RESULT						
2.1	NULL	m	m	m	m		

A.1.3.10 ChangeCredentials

Ref	Element	UA		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	old-credentials	m	m	m	m		
1.1.1	simple	m	m	m	m		
1.1.1.1	octet-string	o	m	o	m		
1.1.1.2	ia5-string	o	o	o	o		
1.1.2	strong	o	o	o	o		
1.1.2.1	bind-token	m	m	m	m		see A.1.9/9
1.1.2.2	certificate	o	o	o	o		
1.2	new-credentials	m	m	m	m		
1.2.1	simple	m	m	m	m		
1.2.1.1	octet-string	o	m	o	m		
1.2.1.2	ia5-string	o	o	o	o		
1.2.2	strong	o	o	o	o		
1.2.2.1	bind-token	m	m	m	m		see A.1.9/9
1.2.2.2	certificate	o	o	o	o		
2	RESULT						

2.1	NULL	m	m	m	m		

A.1.3.11 AMH14 Register

This classification applies only to the AMH14 context. (The AMH12 register operation is specified in A.1.3.9)

Ref	Element	UA		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	user-name	o	o	o	o		see A.1.10.b
1.2	user-address	o	o	o	o		
1.3	deliverable-class	o	o	o	o		
1.3.1	content-types	o	o	o	o		
1.3.2	maximum-content-length	o	o	o	o		
1.3.3	acceptable-encoded-information-types-constraints	o	o	o	o		
1.3.3.1	unacceptable-eits	o	m	m	m		
1.3.3.2	acceptable-eits	o	m	m	m		
1.3.3.3	exclisevly-acceptable-eits	o	m	m	m		
1.3.4	security-labels	o	o	o	o		
1.3.5	extensions	o	o	o	o		
1.4	default-delivery-controls	o	o	o	o		
1.4.1	permissible-operations	o	o	o	m		
1.4.2	permissible-maximum-content-length	o	o	o	m		
1.4.3	permissible-lowest-priority	o	o	o	m		
1.4.4	permissible-content-types	o	o	o	m		
1.4.5	permissible-encoded-information-types	o	o	o	m		
1.4.5.1	unacceptable-eits	o	m	o	m		
1.4.5.2	acceptable-eits	o	m	o	m		
1.4.5.3	exclusively-acceptable-eits	o	o	o	o		

1.5	redirections	o	o	o	o		
1.5.1	redirections-classes	o	o	o	o		
1.5.1.1	content-types	o	o	o	o		
1.5.1.2	maximum-content-length	o	o	o	o		
1.5.1.3	acceptable-encoded-information-types-constraints	o	o	o	o		
1.5.1.3.1	unacceptable-eits	o	m	o	m		
1.5.1.3.2	acceptable-eits	o	m	o	m		
1.5.1.3.3	exclusively-acceptable-eits	o	m	o	m		
1.5.1.4	security-labels	o	o	o	o		see A.1.9/3
1.5.1.5	priority	o	o	o	o		
1.5.1.6	objects	o	o	o	m		
1.5.1.6.1	messages	o	o	o	o		
1.5.1.6.2	reports	o	o	o	o		
1.5.1.6.3	both	o	o	o	m		
1.5.1.7	applies-only-to	o	o	o	o		
1.5.1.8	extensions	o	o	o	o		
1.5.2	recipient-assigned-alternate-recipient	o	m	o	m		
1.6	redirected-delivery	o	o	o	o		see A.1.8/6
1.7	retrieve-registrations	o	o	o	o		
1.7.1	standard-parameters	o	m	o	m		
1.7.1.1	user-name	o	c1	o	c1		
1.7.1.2	user-address	o	c1	o	c1		
1.7.1.3	deliverable-class	o	c1	o	c1		
1.7.1.4	default-delivery-controls	o	c1	o	c1		
1.7.1.5	redirections	o	c1	o	c1		
1.7.1.6	restricted-delivery	o	c1	o	c1		
1.7.2	extensions	o	c1	o	c1		

1.8	extensions	o	o	o	o		
2	RESULT						
2.1	empty-result	o	m	o	m		
2.2	non-empty-result	o	c2	o	c2		
2.2.1	registered information	o	m	o	m		
2.2.1.1	user-name	o	o	o	o		see A.1.10
2.2.1.2	user-address	o	o	o	o		
2.2.1.3	deliverable-class	o	c3	o	c3		
2.2.1.3.1	content-types	o	c3	o	c3		
2.2.1.3.2	maximum-content-length	o	c3	o	c3		
2.2.1.3.3	acceptable-encoded-information-types-constraints	o	c3	o	c3		
2.2.1.3.3.1	unacceptable-eits	o	m	o	m		
2.2.1.3.3.2	acceptable-eits	o	m	o	m		
2.2.1.3.3.3	exclusively-acceptable-eits	o	m	o	m		
2.2.1.3.4	security-labels	o	c3	o	c3		
2.2.1.3.5	extensions	o	c3	o	c3		
2.2.1.4	default-delivery-controls	o	c3	o	c3		
2.2.1.4.1	restrict	o	-	o	-		
2.2.1.4.2	permissible-operations	o	c3	o	c3		
2.2.1.4.3	permissible-maximum-content-length	o	c3	o	c3		
2.2.1.4.4	permissible-lowest-priority	o	c3	o	c3		
2.2.1.4.4	permissible-content-types	o	c3	o	c3		
2.2.1.4.6	permissible-encoded-information-types	o	c3	o	c3		
2.2.1.4.6.1	unacceptable-eits	o	m	o	m		
2.2.1.4.6.2	acceptable-eits	o	m	o	m		
2.2.1.4.6.3	exclusively-acceptable-eits	o	o	o	o		
2.2.1.5	redirections	o	c3	o	c3		

2.2.1.5.1	redirections-classes	o	c3	o	c3		
2.2.1.5.1.1	content-types	o	c3	o	c3		
2.2.1.5.1.2	maximum-content-length	o	c3	o	c3		
2.2.1.5.1.3	acceptable-encoded-information-types-constraints	o	c3	o	c3		
2.2.1.5.1.3.1	unacceptable-eits	o	m	o	m		
2.2.1.5.1.3.2	acceptable-eits	o	m	o	m		
2.2.1.5.1.3.3	exclusively-acceptable-eits	o	m	o	m		
2.2.1.5.1.4	security-labels	o	c3	o	c3		
2.2.1.5.1.5	priority	o	c3	o	c3		
2.2.1.5.1.6	objects	o	m	o	m		
2.2.1.5.1.6.1	messages	o	o	o	o		
2.2.1.5.1.6.2	reports	o	o	o	o		
2.2.1.5.1.6.3	both	o	m	o	m		
2.2.1.5.1.7	applies-only-to	o	c3	o	c3		
2.2.1.5.1.8	extensions	o	c3	o	c3		
2.2.1.5.2	recipient-assigned-alternate-recipient	o	m	o	m		
2.2.1.6	redirected-delivery	o	c3	o	c3		see A.1.8/6
2.2.1.7	extensions	o	c3	o	c3		
2.2.2	extensions	o	o	o	o		

c1 - if the corresponding attribute is supported as an argument then o else not applicable.

c2 - If item 1.7 is supported then m else o.

c3 - if the corresponding attribute is supported as an argument then m else not applicable.

A.1.4 MessageSubmissionEnvelope

Ref	Element	UA		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	originator-name	m	m	m	m		see A.1.10.b
2	original-encoded-information-types	m	m	m	m-		see A.1.8/3
3	content-type	m	m	m	m-		
4	content-identifier	o	o	m	m		
5	priority	m	m	m	m		
6	per-message-indicators	m	m	m	m		see A.1.8/5
7	deferred-delivery-time	o	o	m	m		
8	extensions	m	m	m	m		see A.1.9/1
8.1	recipient-reassignment-prohibited	o	m1	o	m		
8.2	dl-expansion-prohibited	o	m1	o	m		
8.3	conversion-with-loss-prohibited	o	o	o	m		
8.4	latest-delivery-time	o	o	o	o		
8.5	originator-return-address	o	o	o	o		see A.1.10.a
8.6	originator-certificate	o	o	o	o		
8.7	content-confidentiality-algorithm-identifier	o	o	o	o		
8.8	message-origin-authentication-check	o	o	o	o		see A.1.9/2
8.9	message-security-label	o	o	o	o		see A.1.9/3
8.10	proof-of-submission-request	o	i	o	i		
8.11	content-correlator	o	o	m	m		
8.12	PrivateExtensions	c2	c3	c2	c3		
9	per-recipient-fields	m	m	m	m		
9.1	recipient-name	m	m	m	m		see A.1.10.a
9.2	originator-report-request	m	m	m	m		
9.3	explicit-conversion	o	o	o	m-		

9.4	extensions	m	m	m	m		see A.1.9/1
9.4.1	originator-requested-alternate-recipient	o	o	o	o		see A.1.10.a
9.4.2	requested-delivery-method	o	o	o	o		
9.4.3	physical-forwarding-prohibited	o	o	o	o		
9.4.4	physical-forwarding-address-request	o	o	o	o		
9.4.5	physical-delivery-modes	o	o	o	o		
9.4.6	registered-mail-type	o	o	o	o		
9.4.7	recipient-number-for-advice	o	o	o	o		
9.4.8	physical-rendition-attributes	o	o	o	o		
9.4.9	physical-delivery-report-request	o	o	o	o		
9.4.10	message-token	o	o	o	o		see A.1.9/4
9.4.11	content-integrity-check	o	o	o	o		
9.4.12	proof-of-delivery-request	o	o	o	o		
9.4.13	PrivateExtensions	c2	c3	c2	c3		

m1 - only the capability to generate the "prohibited" value is required

c2 - if any access-94 application context is supported (A.1.1 items 5, 6, 7 or 8) then o else –

c3 - if conformance to AMH14 is claimed then o else –

A.1.5 ProbeSubmissionEnvelope

Ref	Element	UA		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	originator-name	m	m	m	m		see A.1.10.b
2	original-encoded-information-types	m	m	m	m-		see A.1.8/3
3	content-type	m	m	m	m-		
4	content-identifier	o	o	m	m		
5	content-length	o	m	m	m		
6	per-message-indicators	m	m	m	m		see A.1.8/5
7	extensions	m	m	m	m		see A.1.9/1
7.1	recipient-reassignment-prohibited	o	m1	o	m		

7.2	dl-expansion-prohibited	o	m1	o	m		
7.3	conversion-with-loss-prohibited	o	o	o	m		
7.4	originator-certificate	o	o	o	o		
7.5	message-security-label	o	o	o	o		see A.1.9/3
7.6	content-correlator	o	o	m	m		
7.7	probe-origin-authentication-check	o	o	o	o		see A.1.9/5
7.8	PrivateExtensions	c2	c3	c2	c3		
8	per-recipient-fields	m	m	m	m		
8.1	recipient-name	m	m	m	m		see A.1.10.a
8.2	originator-report-request	m	m	m	m		
8.3	explicit-conversion	o	o	o	m-		
8.4	extensions	m	m	m	m		see A.1.9/1
8.4.1	originator-requested-alternate-recipient	o	o	o	o		see A.1.10.a
8.4.2	requested-delivery-method	o	o	o	o		
8.4.3	physical-rendition-attributes	o	o	o	o		
8.4.4	PrivateExtensions	c2	c3	c2	c3		

m1 - only the capability to generate the "prohibited" value is required

c2 - if any access-94 application context is supported (A.1.1 items 5, 6, 7 or 8) then o else –

c3 - if conformance to AMH14 is claimed then o else –

A.1.6 MessageDeliveryEnvelope

Ref	Element	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	message-delivery-identifier	m	m	m	m		see A.1.8/1
2	message-delivery-time	m	m	m	m		
3	other-fields	m	m	m	m		
3.1	content-type	m	m	m	m		
3.2	originator-name	m	m	m	m		see A.1.10.a
3.3	original-encoded-information-types	m	m	m	m		see A.1.8/3

3.4	priority	m	m	m	m		
3.5	delivery-flags	m	m	m	m		
3.5.1	implicit-conversion-prohibited	m	m	m	m		
3.6	other-recipient-names	m	m	m	m		see A.1.10.b
3.7	this-recipient-name	m	m	m	m		see A.1.10.a
3.8	originally-intended-recipient-name	m	m	m	m		see A.1.10.a
3.9	converted-encoded-information-types	m	m	m	m		see A.1.8/3
3.10	message-submission-time	m	m	m	m		
3.11	content-identifier	o	m	m	m		
3.12	extensions	m	m	m	m		see A.1.9/1
3.12.1	conversion-with-loss-prohibited	o	o	o	m		
3.12.2	requested-delivery-method	o	o	o	o		
3.12.3	physical-forwarding-prohibited	o	o	o	o		
3.12.4	physical-forwarding-address-request	o	o	o	o		
3.12.5	physical-delivery-modes	o	o	o	o		
3.12.6	registered-mail-type	o	o	o	o		
3.12.7	recipient-number-for-advice	o	o	o	o		
3.12.8	physical-rendition-attributes	o	o	o	o		
3.12.9	originator-return-address	o	o	o	o		
3.12.10	physical-delivery-report-request	o	o	o	o		
3.12.11	originator-certificate	o	o	o	o		
3.12.12	message-token	o	o	o	o		see A.1.9/4
3.12.13	content-confidentiality-algorithm-identifier	o	o	o	o		
3.12.14	content-integrity-check	o	o	o	o		
3.12.15	message-origin-authentication-check	o	o	o	o		see A.1.9/2
3.12.16	message-security-label	o	o	o	o		see A.1.9/3
3.12.17	proof-of-delivery-request	o	o	o	o		

3.12.18	redirection-history	o	o	m	m		
3.12.19	dl-expansion-history	o	o	m	m		
3.12.20	trace-information	c1	c2	c1	c2		
3.12.21	internal-trace-information	c1	c2	c1	c2		
3.12.22	PrivateExtensions	c1	c2	c1	c2		

c1 - if any access-94 application context is supported (A.1.1 items 5, 6, 7 or 8) then o else –

c2 - if conformance to AMH14 is claimed then o else –

A.1.7 ReportDeliveryEnvelope

Ref	Element	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	subject-submission-identifier	m	m	m	m		see A.1.8/1
2	content-identifier	o	c1	m	m		
3	content-type	m	m	m	m		
4	original-encoded-information-types	m	m	m	m		see A.1.8/3
5	extensions	m	m	m	m		see A.1.9/1
5.1	message-security-label	o	c1	o	o		see A.1.9/3
5.2	content-correlator	o	c1	m	m		
5.3	originator-and-DL-expansion-history	m	m	m	m		
5.4	reporting-DL-name	o	m	o	m		see A.1.10.a
5.5	reporting-MTA-certificate	o	o	o	o		
5.6	report-origin-authentication-check	o	o	o	o		see A.1.9/8
5.7	trace-information	c2	c4	c2	c4		
5.8	internal-trace-information	c2	c4	c2	c4		
5.9	PrivateExtensions	c2	c4	c2	c4		
5.10	redirection-history	c2	c4	c3	c5		
6	per-recipient-fields	m	m	m	m		
6.1	actual-recipient-name	m	m	m	m		see A.1.10.a
6.2	delivery	m	m	m	m		

6.2.1	message-delivery-time	m	m	m	m		
6.2.2	type-of-MTS-user	m	m	m	m		
6.3	non-delivery	m	m	m	m		
6.3.1	non-delivery-reason-code	m	m	m	m		
6.3.2	non-delivery-diagnostic-code	o	m	m	m		
6.4	converted-encoded-information-types	m	m	m	m		see A.1.8/3
6.5	originally-intended-recipient-name	m	m	m	m		see A.1.10.a
6.6	supplementary-information	o	o	o	m		
6.7	extensions	m	m	m	m		see A.1.9/1
6.7.1	redirection-history	o	o	m	m		
6.7.2	physical-forwarding-address	o	c1	o	o		
6.7.3	recipient-certificate	o	o	o	o		
6.7.4	proof-of-delivery	o	c1	o	c1		see A.1.9/6
6.7.5	PrivateExtensions	c2	c4	c2	c4		

c1 - if supported in message submission envelope then m else i

c2 - if any access-94 application context is supported (A.1.1 items 5, 6, 7 or 8) then o else –

c3 - if any access-94 application context is supported (A.1.1 items 5, 6, 7 or 8) then m else o

c4 - if conformance to AMH14 is claimed then o else –

c5 - if conformance to AMH14 is claimed then m else –

A.1.8 Common data types

Ref	Element	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	MTSIdentifier						
1.1	global-domain-identifier	m	m	m	m		see A.1.8/2
1.2	local-identifier	m	m	m	m		
2	GlobalDomainIdentifier						
2.1	country-name	m	m	m	m		

2.2	administration-domain-name	m	m	m	m		
2.3	private-domain-identifier	m	m	m	m		
3	EncodedInformationTypes						
3.1	built-in-encoded-information-types	m	m	m	m		
3.2	(non-basic parameters)	o	o	o	o		
3.3	extended-encoded-information-types	m	m	m	m		
4	ContentType						
4.1	built-in	o	o	o	m		
4.2	extended	o	o	o	m		
5	PerMessageIndicators						
5.1	disclosure-of-other-recipients	o	o	m	m		
5.2	implicit-conversion-prohibited	m	m	m	m		
5.3	alternate-recipient-allowed	o	o	m	m		
5.4	content-return-request	o	o	o	o		
5.5	reserved	o	o	o	m-		
5.6	bit-5	o	o	o	m-		
5.7	bit-6	o	o	o	m-		
5.8	service-message	o	o	o	m-		
6	Restricted						
6.1	permitted	o	m	o	m		
6.2	source-type	o	c1	o	m		
6.2.1	originated-by	o	m	o	m		
6.2.2	redirected-by	o	m	o	m		
6.2.3	dl-expanded-by	o	m	o	m		
6.3	source-name	o	m	o	m		
6.3.1	exact-match	o	m	o	m		

6.3.2	pattern-match	o	m	o	m		

c1 - If the restricted applies on an argument then optional.
If the restricted applies on a result and the corresponding attribute is supported in the argument, then mandatory else not applicable.

A.1.9 Extension data types

Ref	Element	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	ExtensionField						
1.1	type	o	m	m	m		
1.1.1	standard-extension	m	m	m	m		
1.1.2	private-extension	o	o	o	m-		see A.3.6
1.2	criticality	m	m	m	m		
1.3	value	m	m	m	m		
2	MessageOriginAuthenticationCheck						
2.1	algorithm-identifier	m	m	m	m		
2.2	content	m	m	m	m		
2.3	content-identifier	o	m	o	m		
2.4	message-security-label	o	m	o	m		see A.1.9/3
3	SecurityLabel						also named message security label
3.1	security-policy-identifier	o	o	o	m-		
3.2	security-classification	o	o	o	m-		
3.3	privacy-mark	o	o	o	m-		
3.4	security-categories	o	o	o	m-		
4	MessageToken						
4.1	token-type-identifier	m	m	m	m		
4.2	asymmetric-token	m	m	m	m		
4.2.1	signature-algorithm-identifier	m	m	m	m		

4.2.2	name	m	m	m	m		
4.2.3	time	m	m	m	m		
4.2.4	signed-data	o	o	o	m-		
4.2.4.1	content-confidentiality-algorithm-identifier	o	o	o	m-		
4.2.4.2	content-integrity-check	o	o	o	m-		
4.2.4.3	message-security-label	o	o	o	m-		see A.1.9/3
4.2.4.4	proof-of-delivery-request	o	o	o	m-		
4.2.4.5	message-sequence-number	o	o	o	m-		
4.2.5	encryption-algorithm-identifier	o	o	o	m-		
4.2.6	encrypted-data	o	o	o	m-		
4.2.6.1	content-confidentiality-key	o	o	o	m-		
4.2.6.2	content-integrity-check	o	o	o	m-		
4.2.6.3	message-security-label	o	o	o	m-		see A.1.9/3
4.2.6.4	content-integrity-key	o	o	o	m-		
4.2.6.5	message-sequence-number	o	o	o	m-		
5	ProbeOriginAuthenticationCheck						
5.1	algorithm-identifier	m	m	m	m		
5.2	content-identifier	o	m	o	m		
5.3	message-security-label	o	m	o	m		see A.1.9/3
6	ProofOfDelivery						
6.1	algorithm-identifier	m	m	m	m		
6.2	delivery-time	m	m	m	m		
6.3	this-recipient-name	m	m	m	m		see A.1.10.a
6.4	originally-intended-recipient-name	o	o	o	m		see A.1.10.a
6.5	content	m	m	m	m		
6.6	content-identifier	o	m	o	m		
6.7	message-security-label	o	m	o	m		see A.1.9/3

7	ProofOfSubmission						
7.1	algorithm-identifier	m	m	m	m		
7.2	message-submission-envelope	m	m	m	m		
7.3	content	m	m	m	m		
7.4	message-submission-identifier	m	m	m	m		
7.5	message-submission-time	m	m	m	m		
8	ReportOriginAuthenticationCheck						
8.1	algorithm-identifier	m	m	m	m		
8.2	content-identifier	o	m	o	m		
8.3	message-security-label	o	m	o	m		see A.1.9/3
8.4	per-recipient	m	m	m	m		
8.4.1	actual-recipient-name	m	m	m	m		see A.1.10.a
8.4.2	originally-intended-recipient-name	o	m	o	m		see A.1.10.a
8.4.3	delivery	o	m	o	m		
8.4.3.1	message-delivery-time	m	m	m	m		
8.4.3.2	type-of-MTS-user	m	m	m	m		
8.4.3.3	recipient-certificate	o	m	o	m		
8.4.3.4	proof-of-delivery	o	m	o	m		see A.1.9/6
8.4.4	non-delivery	o	m	o	m		
8.4.4.1	non-delivery-reason-code	m	m	m	m		
8.4.4.2	non-delivery-diagnostic-code	o	m	o	m		
9	BindToken	m	m	m	m		
9.1	signature-algorithm-identifier	m	m	m	m		
9.2	name	m	m	m	m		
9.3	time	m	m	m	m		
9.4	signed-data	o	o	o	o		
9.5	encryption-algorithm-identifier	o	o	o	o		

9.6	encrypted-data	o	o	o	o		

A.1.10 OR-names

Table A.1.10.a - OR-name forms for identification of remote MTS-user

Ref	OR-Name Form	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	mnemonic OR-address	m	m	m	m-		see A.1.10.1
2	numeric OR-address	o	o	m	m-		see A.1.10.2
3	terminal OR-address	o	o	m	m-		see A.1.10.3
4	formatted postal OR-address	o	o	o	m-		see A.1.10.4
5	unformatted postal OR-address	o	o	o	m-		see A.1.10.5
6	directory-name	o	o	o	c1		

c1 - if the Designation of Recipient by Directory Name EoS is supported then m else if the OR-address is also present then m- else o

Table A.1.10.b - OR-name forms for binding to the MTS-user

Ref	OR-Name Form	MTS-user				Support	Notes/References
		Base	Profile				
1	mnemonic OR-address	o	m				see A.1.10.1
2	numeric OR-address	o	o				see A.1.10.2
3	terminal OR-address	o	o				see A.1.10.3
4	formatted postal OR-address	-	-				
5	unformatted postal OR-address	-	-				
6	directory-name	o	o				

NOTE - For the MTA the registration capabilities are stated in table A.3.4.

The following tables shall be completed according to the OR-address forms for which support is claimed above.

A.1.10.1 Mnemonic OR-address

Ref	Element	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	built-in-standard-attributes	m	m	m	m		
1.1	country-name	m	m	m	m		
1.2	administration-domain-name	m	m	m	m		
1.3	private-domain-name	o	m	o	m-		
1.4	organization-name	o	m	o	m-		
1.5	personal-name	o	m	o	m-		
1.5.1	surname	m	m	m	m		
1.5.2	given-name	o	m	o	m-		
1.5.3	initials	o	m	o	m-		
1.5.4	generation-qualifier	o	m	o	m-		
1.6	organizational-unit-names	o	m	o	m-		
2	built-in-domain-defined-attributes	o	m	o	m-		
3	extension-attributes	o	m	o	m-		
3.1	common-name	o	m	o	m-		
3.2	teletex-common-name	o	m	o	m-		
3.3	teletex-organization-name	o	m	o	m-		
3.4	teletex-personal-name	o	m	o	m-		
3.4.1	surname	m	m	m	m		
3.4.2	given-name	o	m	o	m-		
3.4.3	initials	o	m	o	m-		
3.4.4	generation-qualifier	o	m	o	m-		
3.5	teletex-organizational-unit-names	o	m	o	m-		
3.6	teletex-domain-defined-attributes	o	m	o	m-		

A.1.10.2 Numeric OR-address

Ref	Element	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	built-in-standard-attributes	m	m	m	m		
1.1	country-name	m	m	m	m		
1.2	administration-domain-name	m	m	m	m		
1.3	private-domain-name	o	m	o	m-		
1.4	numeric-user-identifier	m	m	m	m		
2	built-in-domain-defined-attributes	o	m	o	m-		
3	extension-attributes	o	m	o	m-		
3.1	teletex-domain-defined-attributes	o	m	o	m-		

A.1.10.3 Terminal OR-address

Ref	Element	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	built-in-standard-attributes	m	m	m	m		
1.1	country-name	o	m	o	m-		
1.2	administration-domain-name	o	m	o	m-		
1.3	network-address	m	m	m	m		
1.4	terminal-identifier	o	m	o	m-		
1.5	private-domain-name	o	m	o	m-		
1.6	organization-name	o	o	o	o		
1.7	personal-name	o	o	o	o		
1.8	organizational-unit-names	o	o	o	o		
2	built-in-domain-defined-attributes	o	m	o	m-		
3	extension-attributes	o	m	o	m-		
3.1	extended-network-address	m	m	m	m		
3.1.1	e163-4-address	c1	c1	o	m-		

3.1.2	psap-address	c1	c1	o	m-		
3.2	terminal-type	o	m	o	m-		
3.3	common-name	o	o	o	o		
3.4	teletex-common-name	o	o	o	o		
3.5	teletex-organization-name	o	o	o	o		
3.6	teletex-personal-name	o	o	o	o		
3.7	teletex-organizational-unit-names	o	o	o	o		
3.8	unformatted-postal-address	o	o	o	o		
3.9	teletex-domain-defined-attributes	o	m	m	m		

c1 At least one of 'the elements e163-4-address' and 'psap-address' shall be supported.

A.1.10.4 Formatted postal OR-address

Ref	Element	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	built-in-standard-attributes	m	m	m	m		
1.1	country-name	m	m	m	m		
1.2	administration-domain-name	m	m	m	m		
1.3	private-domain-name	o	m	o	m-		
2	extension-attributes	m	m	m	m		
2.1	physical-delivery-country-name	m	m	m	m		
2.2	physical-delivery-office-name	o	m	o	m-		
2.3	physical-delivery-office-number	o	m	o	m-		
2.4	physical-delivery-organization-name	o	m	o	m-		
2.5	physical-delivery-personal-name	o	m	o	m-		
2.6	postal-code	m	m	m	m		
2.7	poste-restante-address	o	m	o	m-		
2.8	post-office-box-address	o	m	o	m-		
2.9	pds-name	o	m	o	m-		
2.10	street-address	o	m	o	m-		

2.11	unique-postal-name	o	m	o	m-		
2.12	extension-OR-address-components	o	m	o	m-		
2.13	extension-physical-delivery-address-components	o	m	o	m-		
2.14	local-postal-attributes	o	m	o	m-		

A.1.10.5 Unformatted postal OR-address

Ref	Element	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	built-in-standard-attributes	m	m	m	m		
1.1	country-name	m	m	m	m		
1.2	administration-domain-name	m	m	m	m		
1.3	private-domain-name	o	m	o	m-		
2	extension-attributes	m	m	m	m		
2.1	unformatted-postal-address	m	m	m	m		
2.2	physical-delivery-country-name	m	m	m	m		
2.3	postal-code	m	m	m	m		
2.4	pds-name	o	m	o	m-		

A.2 Optional functional groups

The following requirements are additional to those specified in A.1 if support of the functional group is claimed (references are to the corresponding table entries in A.1).

A.2.1 Conversion (CV)

A.2.1.1 MessageSubmissionEnvelope

Ref	Element	Profile	
		UA	MTA
A.1.4/9.3	explicit-conversion		c1

c1 - if implicit conversion is not supported (see A.3.3/2) then m else m-

A.2.1.2 ProbeSubmissionEnvelope

Ref	Element	Profile	
		UA	MTA
A.1.5/8.3	explicit-conversion		c1

c1 - if implicit conversion is not supported (see A.3.3/2) then m else m-

A.2.2 Distribution List (DL)

There are no additional requirements for support of protocol elements for support of the DL FG. However, MTAs shall meet the requirements specified in subclause 7.2 of ISO/IEC ISP 10611-1.

A.2.3 Physical Delivery (PD)

The support requirements specified below are for a UA and for an MTA on submission, and for an MTA with a co-located PDAU on delivery, as appropriate.

A.2.3.1 MessageSubmissionEnvelope

Ref	Element	Profile	
		UA	MTA
A.1.4/8.5	originator-return-address		m
A.1.4/9.4.3	physical-forwarding-prohibited	m	m
A.1.4/9.4.4	physical-forwarding-address-request		m
A.1.4/9.4.5	physical-delivery-modes	m	m
A.1.4/9.4.6	registered-mail-type		m
A.1.4/9.4.7	recipient-number-for-advice		m
A.1.4/9.4.8	physical-rendition-attributes		m
A.1.4/9.4.9	physical-delivery-report-request		m

A.2.3.2 ProbeSubmissionEnvelope

Ref	Element	Profile	
		UA	MTA
A.1.5/8.4.3	physical-rendition-attributes		m

A.2.3.3 MessageDeliveryEnvelope

Ref	Element	Profile	
		PDAU	MTA
A.1.6/3.12.3	physical-forwarding-prohibited	m	m
A.1.6/3.12.5	physical-delivery-modes		m
A.1.6/3.12.8	physical-rendition-attributes		m
A.1.6/3.12.10	physical-delivery-report-request		m

A.2.3.4 ReportDeliveryEnvelope

Ref	Element	Profile	
		MTS-user	MTA
A.1.7/6.7.2	physical-forwarding-address		m

A.2.3.5 OR-names

Ref	OR-Address Form	Profile	
		MTS-user	MTA
A.1.10.a/4	formatted postal OR-address	m	m
A.1.10.a/5	unformatted postal OR-address	m	m

A.2.3.5.1 Formatted postal OR-address

Ref	OR-Address Form	Profile	
		MTS-user	MTA
A.1.10.4/2.2	physical-delivery-office-name		m
A.1.10.4/2.3	physical-delivery-office-number		m
A.1.10.4/2.4	physical-delivery-organization-name		m
A.1.10.4/2.5	physical-delivery-personal-name		m
A.1.10.4/2.7	poste-restante-address		m
A.1.10.4/2.8	post-office-box-address		m
A.1.10.4/2.9	pds-name		m

A.1.10.4/2.10	street-address		m
A.1.10.4/2.11	unique-postal-name		m
A.1.10.4/2.12	extension-OR-address-components		m
A.1.10.4/2.13	extension-physical-delivery-address-components		m
A.1.10.4/2.14	local-postal-attributes		m

A.2.3.5.2 Unformatted postal OR-address

Ref	OR-Address Form	Profile	
		MTS-user	MTA
A.1.10.5/2.4	pds-name		m

A.2.4 Redirection (RED)

A.2.4.1 MessageSubmissionEnvelope

Ref	Element	Profile	
		UA	MTA
A.1.4/9.4.1	originator-requested-alternate-recipient		m

A.2.4.2 ProbeSubmissionEnvelope

Ref	Element	Profile	
		UA	MTA
A.1.5/8.4.1	originator-requested-alternate-recipient		m

A.2.5 Latest Delivery (LD)

A.2.5.1 MessageSubmissionEnvelope

Ref	Element	Profile	
		UA	MTA
A.1.4/8.4	latest-delivery-time	m	m

A.2.6 Return of Content (RoC)

A.2.6.1 Operation arguments/results

A.2.6.1.1 Report Delivery

Ref	Element	Profile	
		MTS-user	MTA
A.1.3.7/1.2	returned-content	m	m

A.2.6.2 Common data types

Ref	Element	Profile	
		UA	MTA
A.1.8/5	PerMessageIndicators		
A.1.8/5.4	content-return-request	m	m

A.2.7 Security (SEC)

The support requirements for all SEC classes are as specified in A.1 unless otherwise specified below. Elements classified as cC shall be treated as m if support of a confidential security class variant (SnC) is claimed, else as o.

A.2.7.1 Supported operations

A.2.7.1.1 Message Submission Service Element (MSSE)

Ref	Element	MTS-user			MTA		
		S0	S1	S2	S0	S1	S2
A.1.2.2/4	SubmissionControl				m	m	m

A.2.7.1.2 Message Delivery Service Element (MDSE)

Ref	Element	MTS-user			MTA		
		S0	S1	S2	S0	S1	S2
A.1.2.3/3	DeliveryControl		m	m			

A.2.7.2 Operation arguments/results

A.2.7.2.1 MTSBind

Ref	Element	MTS-user			MTA		
		S0	S1	S2	S0	S1	S2
A.1.3.1/1.3	initiator-credentials	mr	mr	mr	mr	mr	mr
A.1.3.1/1.3.1	simple		ix	ix		ix	ix
A.1.3.1/1.3.2	strong		mr	mr		mr	mr
A.1.3.1/1.3.2.1.4	signed-data		mr	mr		mr	mr
A.1.3.1/1.4	security-context		mr	mr		mr	mr
A.1.3.1/2.3	responder-credentials	mr	mr	mr	mr	mr	mr
A.1.3.1/2.3.1	simple		ix	ix		ix	ix
A.1.3.1/2.3.2	strong		mr	mr		mr	mr
A.1.3.1/2.3.2.1.4	signed-data		mr	mr		mr	mr

A.2.7.2.2 MessageSubmission

Ref	Element	UA			MTA		
		S0	S1	S2	S0	S1	S2
A.1.3.2/2.4.1	originating-MTA-certificate	ix	ix	o	ix	ix	o
A.1.3.2/2.4.2	proof-of-submission	ix	ix	m	ix	ix	m

A.2.7.2.3 SubmissionControl

Ref	Element	UA			MTA		
		S0	S1	S2	S0	S1	S2
A.1.3.5/1.1.2	permissible-operations				m	m	m
A.1.3.5/1.1.3	permissible-maximum-content-length				m	m	m
A.1.3.5/1.1.4	permissible-lowest-priority				m	m	m
A.1.3.5/1.1.5	permissible-security-context		m	m		m	m